

Department of the Navy Headquarters Network (DNHN)

- VERSION 1 -

Standards, Policies and Procedures For DNHN

24 February 1998



**Department of the Navy
Information Network Program Office**

TABLE OF CONTENTS

SECTION I	INTRODUCTION.....	1
1.1	OVERVIEW	1
SECTION II	DNHN SUPPORT POLICIES & PROCEDURES.....	2
2.1	OVERVIEW	2
2.2	HOURS OF OPERATION.....	2
2.3	CRC PROCEDURES.....	2
2.4	OPENING AND CLOSING LAN AND E-MAIL ACCOUNTS; PASSWORD CHANGES.....	2
2.5	DNHN STANDARD NETWORK CONFIGURATION	2
SECTION III:	REQUIRMENTS FOR PROCUREMENT AND PROJECTS.....	5
4.1	OVERVIEW	7
4.2	PASSWORDS	7
4.3	PHYSICAL SECURITY	8
4.4	INFORMATION SECURITY	10
4.5	SOFTWARE VIRUS PROTECTION.....	11
4.6	SECURITY ENFORCEMENT AND REPORTING SECURITY VIOLATIONS.....	13
4.7	COPYING FILES BETWEEN CLASSIFIED AND UNCLASSIFIED LANS.....	13
SECTION V:	CONFIGURATION MANAGEMENT.....	14
5.1	OVERVIEW	14
5.2	HARDWARE AND SOFTWARE CONFIGURATIONS ON WORKSTATIONS	14
SECTION VI:	COMPUTER TRAINING.....	15
6.1	OVERVIEW	15
6.2	ELIGIBILITY.....	15
6.3	REGISTRATION.....	15
6.4	COURSE INFORMATION.....	15
SECTION VII:	ELECTRONIC MAIL.....	16
7.1	UNCLASSIFIED MAIL ACCOUNTS	16
7.2	UNCLASSIFIED POST OFFICE MAINTENANCE.....	16
7.3	PUBLIC FOLDERS AND BULLETIN BOARDS	17
7.4	REMOTE ACCESS TO THE DNHN UNCLASSIFIED LAN MAIL ACCOUNTS	17
7.5	CLASSIFIED MAIL ACCOUNTS.....	17
7.6	DNHN CLASSIFIED MAIL ADDRESS.....	18
7.7	CLASSIFIED NAVAL MESSAGE BULLETIN BOARDS.....	18
7.8	GENERAL INFORMATION MESSAGES.....	18
7.9	DNHN CLASSIFIED POST OFFICE MAINTENANCE.....	19
7.10	CLASSIFIED INACTIVE E-MAIL ACCOUNTS	19
7.11	REMOTE ACCESS TO THE CLASSIFIED LAN MAIL ACCOUNTS	19
SECTION VIII:	DNHN LAN MAINTENANCE & ADMINISTRATION	20
8.1	LAN SERVER SCHEDULED MAINTENANCE.....	20
SECTION IX	REMOTE DIAL-IN POLICIES & PROCEDURES.....	23
9.1	REMOTE FUNCTIONS SUPPORTED.....	23
9.2	ESTABLISHING AN ACCOUNT.....	23

APPENDIX A:	DNHN QUICK START GUIDE.....	24
APPENDIX B:	FREQUENTLY ASKED QUESTIONS.....	50
APPENDIX C:	MEMORANDUM OF AGREEMENT FOR USER ACCESS TO DNHN COMPUTER SYSTEMS.....	53
APPENDIX D:	LOCAL AREA NETWORK (LAN) SECURITY BRIEFING OUTLINE	56
APPENDIX E:	FILE TRANSFER PROCEDURES FOR COPYING FILES BETWEEN CLASSIFIED AND UNCLASSIFIED LANS.....	58
APPENDIX F:	REQUIREMENTS PROCESS--THREE-YEAR POM	61
APPENDIX G:	REQUIREMENTS PROCESS—ANNUAL BASIS.....	62
APPENDIX H:	REQUIREMENTS PROCESS--EMERGENT REQUIREMENTS.....	63

SECTION I INTRODUCTION

1.1 Overview

This document provides users a single source of reference for policies, procedures, and standards that apply to the Department of the Navy Headquarters Network (DNHN). Its intent is to improve user information technology infrastructure support by specifying user and system administrator responsibilities; documenting maintenance support procedures; and providing information on the processes used to implement system improvements.

The Department of the Navy Information Network Program Office (DoN INPO) is responsible for managing the DNHN and for keeping this document current.

SECTION II DNHN SUPPORT POLICIES & PROCEDURES

2.1 Overview

The Customer Response Center (CRC) is normally the first contact point for Information Technology (IT) support services to all users of the DNHN. The CRC's telephone number is (202) 444-0600.

2.2 Hours of Operation

The normal hours of operation for the CRC are 24 hours a day, 7 days a week.

2.3 CRC Procedures

All telephone calls and e-mail requests to the CRC are received by CRC representatives. To the extent possible, the CRC strives to resolve all issues over the telephone. A computerized trouble ticket is initiated by the CRC for every reported problem. The trouble ticket remains open until the problem is fixed. The user who reports the problem will be informed of the trouble ticket number. This number provides a common reference point between the user and the CRC in subsequent discussions of the problem and its resolution status.

2.4 Opening and Closing LAN and E-mail Accounts; Password Changes

User requests for network and e-mail accounts, password resets, or network connections should be forwarded to the Automated Data Processing Systems Security Office (ADPSSO) or Information Systems Coordinator (ISC) for subsequent coordination with the CRC and DON INPO's security manager.

The organization ADPSSO is responsible for notifying the CRC when an individual reports to an organization and requires an account/password, or when an individual with a DNHN LAN and/or e-mail account departs from the organization. Upon notification of departure, the CRC will then close the account.

2.5 DNHN Standard Network Configuration

DON INPO purchases and maintains a standard set of state-of-the-market computer hardware and software for connection to the DNHN. Normally, organizations with a need for new hardware or software should submit their requirements to their OPNAV or SECNAV requirements officer, who will initiate the requirements process. Organizations that wish to purchase their own hardware or software must coordinate that purchase with DON INPO. Non-standard equipment may create problems on the network, and DON INPO support for that equipment may be limited. All purchases of non-standard hardware and software must be submitted to and be approved by DON INPO's Configuration Control Board.

2.5.1 DNHN Standard Hardware

DNHN standard hardware is defined as any automated data processing equipment that was approved by DON INPO for use on the DNHN and has bar codes. This includes but is not limited to PCs, printers, servers, laptops, and scanners.

2.5.2 DNHN Standard Software

Every workstation connected to the DNHN LAN is initially set up to a standard baseline software configuration. This baselined software is supported by the CRC. Software that is currently supported includes:

- MS Windows95
- MS Word for 95 Version 7
- MS Excel for 95 Version 7
- MS Power Point 95 Version 7
- MS Exchange 4.0
- MS Schedule+ Version 7
- MS Access Version 7
- McAfee Anti-Virus Protection
- MS Internet Explorer Version 3.0
- Lotus Organizer 2.1
- Lotus cc:Mail 2.21
- Lotus cc:Mail Notify 2.0
- MTF Editor 3.5

2.5.3 Non-standard Software

The CRC will create a trouble ticket to assist users with non-standard software packages; however, they normally will not be handled as a high priority. The following software is prohibited for use on the DNHN LAN:

- Any software that DONINPO does not have a legal license to operate.
- Any privately owned software package (e.g., Quicken).
- Any Public Domain/Shareware software package.

All screen savers (unless provided with Windows operating system).

2.5.4 Consumable Computer Supplies

All consumable computer supplies are obtained through the organization's supply system. Those types of supplies include:

- Paper
- Ink ribbons
- Toner cartridges
- Diskettes
- Plotter Pens
- Color Printer supplies
- Overheads
- Screen Cleaner

SECTION III: REQUIRMENTS FOR PROCUREMENT AND PROJECTS

User requirements that are received in the CRC that are non-standard or non-services in nature feed another DON INPO process; i.e., the requirements for procurement and projects process. Requirements are considered on a three-year long-term POM process, an annual basis, and as emergent requirements arise. Appendices F, G, and H are flow diagrams of these three processes. This document explains the execution year plan and emergent requirements process.

The requirements process is designed to give equal representation to the SECNAV and OPNAV users. Both SECNAV and OPNAV have Requirements Officers who approve/disapprove, prioritize and forward requirements to DoN INPO. The Deputy Program Manager (DPM) for Plans, Functional Analysis, and Metrics (PFAM) is the primary liaison between the INPO staff and the Requirements Officers. This document will define the process by which a requirement is “funneled” to DoN INPO for action.

The Process:

1. The user contacts the CRC and identifies a new requirement.
2. The CRC enters the requirement into the trouble ticket data base and provides the user with the trouble ticket number.
3. The CRC forwards the new requirement to the PFAM staff in INPO.
4. The Deputy Program Manager, PFAM assigns a project lead who verifies the requirement with the appropriate Requirements Officer in SECNAV or OPNAV. Requirements Officers are:

SECNAV: Mr. Gary Wyckoff , AAUSN/ADP, 695-8854;
e-mail: wyckoff.gary@hq.navy.mil

OPNAV: CAPT John Sting and CDR Charlie Booth, N-09BC, 614-8418;
e-mail: sting.john@hq.navy.mil; and booth.charles@hq.navy.mil

Mr. Barney Thomson, N-804J, 695-8054; e-mail: thomson.barney@hq.navy.mil

(A User may also e-mail requirements directly to the respective Requirements Officer for entrance into the process. Requirements Officers also hold periodic user representative meetings and initiate data calls for requirements information. An annual data call is conducted prior to execution year and is the basis for execution year allocation of products and project initiatives. It serves as a refinement to the POM plan. Emergent requirements are reviewed quarterly by the Requirements Officers and INPO staff.)

5. The Requirements Officers validate requirements with the following possible outcomes.
 - a. If a requirement is valid, the Requirements Officer will determine and assign the **ticket** with the priority of the new requirement.
 - b. If the requirement is determined not to be valid, the Requirements Officer will inform the user and update the ticket, notifying the PFAM project lead to close the ticket.
6. Once a requirement has been validated and determined to have a high priority, the PFAM project lead will perform a functional analysis and coordinate the procurement and/or engineering project with the INPO Engineering and Architecture, Resource Management and Logistics, and Systems Maintenance and Operations Deputy Program Managers and staffs to obtain engineering alternatives, configuration management approval, resource allocation, procurement, inventory control and deployment.
7. The PFAM project lead will inform the user and the Requirements Officer of any changes to the status of the new requirement.
8. The ticket will be closed in one of the following manners:
 - a. The PFAM project lead will confirm verbally or by email, with the originator of the ticket, that the requirement has been satisfied.
 - b. The PFAM project lead and the originator of the ticket is informed by the Requirements Officer, either verbally or by email, that the requirement is not valid.

The originator of the ticket contacts the CRC, PFAM project lead, or the Requirements Officer verbally or by email, and requests that the new requirement be canceled.

SECTION IV: SECURITY

4.1 Overview

Information Systems (IS) security is the responsibility of each user. Security includes the protection of equipment, software, data, and work spaces. Each organization and N-code IS Site Security Officer (ADPSSO) must ensure that users comply with minimum security program requirements. ADPSSOs are assisted in this task by the Network Security Officer and the Customer Response Center (CRC).

The Department of the Navy (DON) Information Systems (IS) Security Program Instruction (SECNAVINST 5239.3) requires that security procedures for command automated information systems (AIS) are developed, documented, and presented to all users. The Information Systems Security Plan (draft) dated 11 March 1996 provides information on how those requirements are met for the DNHN. This section outlines user's responsibilities in meeting requirements. User compliance with this document will maximize IS security, and minimize user induced IS hardware and software problems.

The unclassified segment is Sensitive But Unclassified (SBU). The classified segment of the DNHN is a SECRET HIGH System.

Compliance with applicable IS security regulations is mandatory. Non-compliance with IS security policy and regulations constitutes a security violation. A Memorandum of Agreement (MOA) for User Access to DNHN Computer Systems (Appendix C) form shall be signed by all users and kept on file by the organization's ADPSSO. Security training and awareness shall be administered by the ADPSSO and completed annually by all LAN users. The Local Area Network (LAN) Security Briefing (Appendix D) contains the topics that must be covered at a minimum during that annual training.

4.2 Passwords

Access to the LAN is controlled by a UserID and a password. Certain LAN applications (e.g., cc:Mail, WINPAT) also limit access by requiring users to have authorized accounts. The LAN and cc:Mail accounts are both identified by their UserID. DNHN Unclassified LAN UserIDs are normally the user's last name and first and middle initials (e.g., JonesBA). DNHN Classified LAN UserIDs are normally the individual's office code.

A password is assigned to UserIDs to meet C2 (for more information on C2 NAVSO Pub 5239.XX) security requirements for system protection. When a new user account is established on the LAN, the system administrator creates his account using a common password. Users should change passwords immediately after logging on for the first time. Subsequent password changes must be made every 90 days for security purposes. Changes can be made more frequently. The user will receive an alert upon system log-in that will advise if password time period is expiring. The user LAN account will be disabled if passwords are not changed within the required period. Users should

never boot workstations from a boot diskette. This circumvents the password process and will not allow access to network resources.

If the user forgets his password, or becomes locked out of the system because the wrong password was entered, the user should contact his/her ADPSSO or ISC to notify the Help Desk to reset the password. If the ADPSSO or the ISC is unavailable, there should be an alternate who can assist. For O-7's and above, the CRC will send a representative to the user's office to accomplish the reset.

All user passwords must conform to the following rules:

- Must be a minimum of six characters.
- Must be changed every 90 days.
- Handle as classified information (must not be shared).
- Change password immediately if compromise is suspected.
- Cannot be reused.
- Meaningless word strings (i.e. railway_wharf; boat_holiday; tissue_rope) are recommended. No persons, places, or things that can be closely identified with a user should be used.

4.3 Physical Security

The following procedures must be followed (at a minimum) by users to ensure the physical security of the LAN and its components:

- Workstations with non-removable fixed hard drives must be in an area cleared for open storage per OPNAVINST 5510.60L (Sergeant & Greenleaf lock and space alarm). Workstations' removable hard disks must be secured in a safe when unattended.
- All computer media (e.g., workstations, printers, scanners, removable hard drives, floppy disks) must be labeled per OPNAVINST 5510.60L(see the following table) to identify the highest level of data classification that it processes or stores. At a minimum, all components connected to the DNHN classified LAN must be classified SECRET (RED label).

Color-coded labels are as follows:

Unclassified - Green
Confidential - Blue
Secret - Red

- Politely challenge and identify people who you don't recognize as belonging in your organizational area. Any unauthorized visitors in your space shall be escorted.
- A list of personnel authorized to use each AIS system (user accounts) shall be maintained by the ADPSSO and should be revised as required to ensure its accuracy.
- The ADPSSO must be notified and the DON INPO Operations group must approve the relocation of any IS systems or components.
- Workstation output (printouts, graphics, etc.) shall be marked with the appropriate classification by the user. Downgrading of the classification is the user's responsibility and requires that the user visually review each page.
- To minimize damage, workstations shall not be placed directly next to wall vents/ under overhead vents, or placed within 18 inches of heat producing devices. Users shall ensure that workstation vents remain clear. Printers shall not be placed on top of workstations due to its vibration, dust, and heat. Food and drinks shall be kept away from IS components and media.
- Each workstation should be connected to a surge suppresser to protect against electrical surges.
- In the event of an emergency evacuation, the user shall comply with the following (time and safety permitting):
 1. Turn off all IS systems and other electrical equipment.
 2. Secure space.
- If a power outage occurs while an IS system is operating, remove any floppy diskettes from the drives and secure the power switch at the surge suppresser.

Firewalls have been implemented to protect the DNHN. There is still a remote possibility of an intrusion from outside of the network. Intrusions from inside of the network can be minimized by users protecting passwords and changing passwords on a regular basis.

Be familiar with the following intrusion symptoms and take action as indicated if an intrusion is suspected.

Intrusion Symptoms

- System slowdown or shutdown for no apparent reason.
- Files or programs are suddenly missing.
- Alteration in file text.
- Sudden unexplained appearance of files.

If you experience any of the above symptoms or suspect that your computer or the LAN has been accessed by someone other than you, take the following actions:

- Stop all operations at that workstation immediately.
- Notify the Help Desk immediately and request assistance.

4.4 Information Security

- Access privileges for sensitive files shall be established and periodically reviewed by the ADPSSO.
- Log off the LAN if you are going to leave your workstation unattended for longer than 30 minutes.
- Use one of the available Windows screen savers to mask your screen when the workstation is not in use.
- Use of modems on the DNHN behind the firewall must be approved by the Designated Approval Authority.
- Sensitive data that does not have password entry control should not be left in the workstation or LAN.
- Conduct a virus check with the LAN Anti Virus utility prior to using any diskette.
- Privately owned computer hardware or software resources shall not be used in work spaces without prior approval of the Network Security Officer or ISSO. Under no circumstances shall classified processing be conducted on privately owned resources.
- All diskettes removed from DNHN Classified LAN shall be considered SECRET due to the SECRET HIGH designation of that network. If the user desires to handle these disks as unclassified, appropriate downgrade procedures must be implemented.
- Diskettes should be stored upright in a dust-free container when not in use.

- All diskettes shall be removed from the workstation when not in use and stored according to classification in properly locked containers. The locked container regulation may be superseded by open storage authorization for vaulted secure work areas. Unclassified media must also be secured to minimize risk of inadvertent loss.
- All media containing Privacy Act data (people's names and social security numbers listed together) shall be secured in a locked desk or file cabinet at the following times:
 1. During non-working hours.
 2. When the information system is left unattended.
 3. When the information system is being operated by an authorized user who doesn't have a need to access Level II data.
- Monitors should not face an outside window or doorway leading to a common hallway.
- Classified Workstations and/or switching devices shall be at least one meter (40") from any sending/receiving device (e.g. non-classified personal computer, telephone, STU-III).
- Workstations shall not be in offices which don't carry a classification of at least the level of the workstation, i.e. a workstation processing Secret information may be placed in a space comprised of Top Secret employees; however, a Secret processing workstation cannot be placed in an office with personnel cleared below Secret.
- Laptop computers are not permitted access or connectivity to the classified LAN without prior approval by the DNHN Designated Approving Authority (DAA).

4.5 Software Virus Protection

A virus is an actively infectious computer program that places copies of itself into other applications and programs, eventually corrupting data files and documents. Software viruses can quickly infect LAN file servers and all connected workstations. They pose a significant threat to files, systems software, and hardware. Prevention, not correction, is the key to successful LAN software virus protection.. McAfee Anti-Virus software has been installed on all the LAN workstations. It is loaded as a Terminate and Stay Resident (TSR) program. The program continually scans computer resources for viruses. When configured correctly, it scans all files from any source as they are opened. A window with an alert notification will appear on your screen if a virus is detected.

Users shall adhere to the following rules to minimize the possibility of virus infections:

- Scan diskettes for viruses before copying files to your workstation or LAN, or running programs from the diskettes.

- Utilize your home directory on the LAN to save critical files. All files in those directories are backed up nightly to facilitate quick recovery in the event of virus attacks. Those files can be accessed from another LAN workstation in the case where the user workstation becomes inoperative.
- Use of new software applications shall be coordinated through the DON INPO Ops group prior to being placed on workstations or the LAN. This includes shareware, public domain software, and any other software not directly obtained from DON INPO or its support staff. Violations of this policy shall be reported to the ADPSSO and the Network Security Officer.
- Write protect program master diskette (original manufacturer's program disks) and never save files to those disks.
- Never boot a hard drive system from a diskette unless required to recover from an inoperative hard drive, conducting virus troubleshooting, or when directed by the CRC or ADPSSO.
- Never boot workstations from a diskette unless it is the original write protected master, or a previously scanned copy. This will prevent boot sector viruses.

Users shall familiarize themselves with the following list of typical virus symptoms:

- System slowdown or shutdown for no apparent reason.
- Out of memory errors.
- Sudden loss of hard disk space.
- Sudden increase in the number of disk sectors marked unusable or bad.
- Files or programs are suddenly missing.
- Unexpected video display or audio/musical noise.
- Massive destruction of data.
- Unexpected change in size or creation date of a program or file.
- A program not responding properly.
- Alteration in file text or commands.
- Unusual error messages.
- Unusual, obscene, or annoying messages on your screen.
- Lost or garbled output to screens or printers.
- Sudden unexplained appearance of files.

- Excessive disk access time.
- Excessive delays in communications or printing tasks.
- Unusual or slow behavior on workstation reboots.

If you experience any of the above symptoms or you detect or suspect that your computer or the LAN has been infected by a virus, take the following actions:

- Stop all operations at that workstation immediately.
- DO NOT turn the infected workstation off!
- Remove any diskettes from the workstation floppy drives and keep them available for CRC personnel to examine.
- Leave the software application running.
- Notify the CRC immediately and request assistance!
- Do not continue to use applications until approval is given by the CRC technician.

4.6 Security Enforcement and Reporting Security Violations

The user is responsible for reporting any damage, destruction, theft, or unauthorized disclosure of any hardware, software, data, or supporting documents. Reports must be filed immediately via the user's ADPSSO. Security incident reporting is an integral part of any IS security plan and will also be reviewed by the ISSO.

ADPSSOs are required to report all security incidents. Incident reports must be submitted to the IS Security Officer in writing within 24 hours of the incident.

4.7 Copying Files between Classified and Unclassified LANs

DNHN users who use both the Classified and Unclassified LANs in their office will often need to copy files from one environment to the other, a daily occurrence which presents the risk of classified information unintentionally moving to the UNCLAS environment. Security regulations prohibit direct physical connection between the LANs; therefore, the standard procedure requires the use of floppy disks in a prescribed manner that ensures that no classified information passes on parts of the media not normally viewed by the user. Please see Appendix E for the file transfer procedures.

SECTION V: CONFIGURATION MANAGEMENT

5.1 Overview

LAN Configuration Management (CM) is an important discipline that must be addressed throughout the DNHN LAN's life-cycle. CM involves the application of technical and administrative direction and surveillance to achieve three purposes:

- To identify and document the functional and physical characteristics of a configuration item (e.g., hardware) or Computer Software Configuration Item (CSCI).
- To control changes to those items.
- To record and report changes in the hardware and software configuration.

The DoN INPO Configuration Control Board (CCB) is led by the Deputy Program Manager for Resource Management and Logistics. The CCB meets weekly to approve changes that have resulted from user requirements or from internal INPO engineering and operational necessity.

5.2 Hardware and Software Configurations on Workstations

5.2.1 Autoexec.Bat & Config.Sys Files

All workstations attached to the DNHN LAN are installed with standardized configuration files which include the Config.Sys and Autoexec.bat files. Those files are set to provide the workstation with maximum memory and performance features. Users shall not make any changes that alter the system configuration. The DNHN Support Staff shall make all required changes to ensure that there is no interference with network programs.

5.2.2 Computer Addresses

Each workstation attached to the DNHN LAN has a unique network software address and computer name. The user's organization (e.g., N6, ASN(M&RA)), room number, and workstation drop number make up the computer name. To prevent LAN conflicts, all changes to the computer address and name shall be coordinated with the DNHN LAN Support Staff. Specifically, users shall not change the location of workstations without coordinating with the CRC.

SECTION VI: COMPUTER TRAINING

6.1 Overview

The DON INPO Computer Training Program provides instruction for navy personnel in the use of standard DNHN office automation software. Classes in word-processing, spreadsheets, graphics, e-mail, and database products are offered free of charge to government personnel associated with the DNHN Classified and Unclassified LANs.

6.2 Eligibility

All personnel (military and civilian) whose billets require access to the DNHN LANs are eligible to attend training classes. Individuals must have the approval of their supervisor prior to registering for training.

6.3 Registration

Personnel must contact their Training Coordinator to fill out a registration form, and then submit that form to the DON INPO Training Coordinator or e-mail request to “CLASSES” (an alias). Personnel not assigned to SECNAV or OPNAV may pick up registration forms outside the Training Room or call (703-693-8100) for more information between 0800-1600. Class registration will be confirmed by their coordinator or the DNHN Training Coordinator upon receipt of the form. Available quotas are filled on a first come first served basis. A standby list will be maintained by the Training Room. In the event of a cancellation, it will be used to fill the open class seats.

6.4 Course Information

Training includes hands-on experience with one microcomputer per person. Completion of an Introductory Course, or equivalent experience, is strongly recommended prior to participation in Intermediate or Advanced Courses. Classes will be conducted in the DNHN Classified Training Center, room 5E562, The Washington Navy Yard, Bldg. 176 Room 200, or at the BTG Training Facility on the Pentagon Concourse. Class hours are from 0830 to 1530, with lunch typically from 1130 to 1230. Classes will start promptly at the time designated. If seats are still open ten minutes after the start of class, standbys will be notified in order of their sign up. If students are unable to attend a scheduled class, the training coordinator and/or the Training Room Administrator (693-8100) must be notified NLT 30 minutes prior to the start of the class.

SECTION VII: ELECTRONIC MAIL

7.1 Unclassified Mail Accounts

The DNHN Unclassified mail system is MS Exchange. The name on the mailbox is the user's last name, first initial, and middle initial.

The storage limit per user on the Unclassified LAN is 20 MB. Users who exceed that limit are prohibited from sending e-mail. Users will begin to get mailbox size warnings every day when mailbox size is at 10 MB or larger. There is no limit at this time for the life span of user accounts. The limit is on the size of mailboxes.

7.1.1 Unclassified User Sent Mail Message Folder

MS Exchange is configured to save your sent mail in the Sent Mail folder. Those messages need to be archived and cleared out periodically because they count against your mailbox size.

7.1.2 Unclassified User Deleted Item Folder

Deleted messages are stored in your Deleted Item folder. This folder is emptied every time you exit MS Exchange

7.1.3 Unclassified User E-mail Inbox

Messages addressed to the user will be posted in the Inbox. When Exchange first opens, it defaults into the user Inbox. Messages are not removed from this folder during LAN maintenance routines. Rather, the user is responsible for ensuring that his or her post office does not exceed the 20 MB limit. Cleaning out the Inbox should be a normal routine.

7.1.4 Unclassified User E-mail Archives

Archives are best kept in Personal folders. Personal folders set up as a “.PST” file on a drive you specify. The archive files appear as folders in your MS Exchange mailbox, but do not count against your 20 MB. For help on setting up archive folders, go to the help section of MS Exchange or call the CRC.

7.2 Unclassified Post Office Maintenance

Periodic maintenance is performed on the Unclassified LAN, during which time access to Exchange may be impacted.

7.3 Public Folders and Bulletin Boards

Public folders and bulletin boards are available for use by the end user. Access rights are determined by the individual's organization.

7.3.1 Unclassified Naval Message Bulletin Boards

Naval messages are posted under Public Folders-All Public Folders-Naval Messages.

7.3.2 Unclassified General Information Messages

General messages are posted for the user community in Public Folders. Information messages are posted in Public Folders-All Public Folders-DNHN Pentagon Public Folders-DNHN Announcements. These messages will be posted to remind users of upcoming network outages or general information regarding the networks. It is the user's responsibility to check on a daily basis for new messages which are posted in their bulletin board.

7.4 Remote Access to the DNHN Unclassified LAN Mail Accounts

Limited remote access to the DNHN unclassified mail accounts is available and can be requested by completing and submitting a request form to your requirements officer. The request form, along with the DNHN dial-in policy, can be found on DNHN's Internet Home Page in the archives section on Remote Dial-In Procedures, <http://www.hq.navy.mil>. In addition, to mail accounts, dial-in users are able to work with network folders and applications, and can also access the Internet.

7.5 Classified Mail Accounts

The DNHN Classified mail system utilizes Lotus cc:Mail version 2.21. The name of the mailbox is the user's organization code. The "comments" field contains the name of the person who is assigned to that code, followed by that person's phone number. The person's name also appears as an entry in the directory with their billet in the comments field. This second entry is actually an "alias" and provides a reverse lookup capability for each user.

The storage limit per user on the Classified LAN (cc:Mail) is 30 days of messages, which includes In-box, Folders, Message Log, and Trash. It does not include archived messages since they are not stored within the post office. Post office maintenance performs deletions automatically of messages older than 30 days in the Inbox and all folders.

7.5.1 Classified User E-mail Message Log

The Classified MESSAGE LOG is a special folder which stores copies of all the user's outgoing e-mail messages. The Classified post office maintenance procedure deletes all Message Log messages that are older than thirty (30) days.

7.5.2 Classified User E-mail Trash

TRASH is a special folder which stores all messages that have been deleted by the user. The post office maintenance procedure deletes all TRASH messages that are older than seven (7) days. This means that deleted messages can only be recovered within 7 days of the user deleting them if the user has not activated the empty trash upon exit rule.

7.5.3 Classified User E-mail In-box

The DNHN Classified e-mail maintenance procedure deletes all Inbox messages older than thirty (30) days. If users wish to keep messages longer than thirty days, they must store them in user created archive files. For messages with file attachments, the file attachments should be saved to disk (home drive is acceptable) and the message should be deleted. (note: all folders are considered part of the Inbox. Maintenance will delete old messages. Only archives are safe).

7.5.4 Classified User E-mail Folders

Users have the capability to create electronic folders in cc:Mail and store messages for future reference in those folders. The folders are stored in the user's mail box in the cc:Mail post office. Messages that are needed for reference for an interim period of time (90 - 180 days) should be stored there by the user.

7.5.5 Classified User E-mail Archives

If the user needs a message for long-term reference (longer than 180 days), he should create an electronic archive in cc:Mail and file the message in the archive. Archives are stored in the user's cc:Mail directory on their home ("H") drive. DON INPO recommends that the user create one archive file for each message folder.

7.6 DNHN Classified Mail Address

Address formats for Classified LAN accounts can be obtained from your ADPSSO.

7.7 Classified Naval Message Bulletin Boards

Naval messages are stored in bulletin boards, created by the CRC for certain users who are given permission to write and by other users who are only authorized to read. They are deleted after five days.

7.8 General Information Messages

All general announcements which affect all personnel (network downtime, policy/procedure changes, conference announcements, requests for volunteers, etc.) are posted to a bulletin board titled "Announcements". It is the user's responsibility to check on a daily basis for new messages which are

posted in their bulletin board.

7.9 DNHN Classified Post Office Maintenance

When the post office is shut down, the message "Post office is temporarily shut down" is displayed. Access to mail is denied until the post office is re-opened. If the maintenance procedure fails for any reason, it is assumed that the post office is not usable and is therefore left shut down until an administrator corrects the problem and reopens the post office. The maintenance procedure runs for approximately one hour, depending on the number of stored messages in the post office. The procedure performs the following functions: deletes 30 day old messages from mailboxes, deletes 5 day old messages from navy message bulletin boards, checks and corrects the integrity of the post office, compacts the message database, and makes a backup copy of the post office.

7.10 Classified Inactive E-mail Accounts

Security regulations prohibit the accumulation of mail in an inactive mailbox. If a billet is vacant, or an e-mail account has not been accessed for 90 days, the e-mail administrator will delete the account. A new account will be established only by request of the ISSSO or ISC in accordance with established procedures.

7.11 Remote Access to the Classified LAN Mail Accounts

Remote access to the DNHN Classified LAN mail network is available via STU-III modem using cc:Mail Remote or cc:Mobile. Any individual who needs remote access must submit a Memorandum Of Agreement (MOA) to the DNHN Designated Approving Authority via DON INPO. The account will be valid for one year from the approval date. Accounts may be renewed by resubmitting a MOA. If the key ID changes for any reason, a letter must be submitted which documents this change in order to re-establish connectivity. To request this connectivity, contact the DNHN Help Desk at 202-433-0600.

SECTION VIII: DNHN LAN MAINTENANCE & ADMINISTRATION

8.1 LAN Server Scheduled Maintenance

Like any piece of machinery, the DNHN requires routine preventative maintenance. The lack of such maintenance will invariably lead to unplanned system “crashes” that may have severe operational impacts. The following sections detail scheduled LAN system maintenance. Users must be familiar with this information, and plan their work schedules accordingly.

8.1.1 Mail Maintenance

Automatic maintenance routine is started for every e-mail post office on the DNHN. The routine includes the cc:Mail Checkstat, Reclaim, Analyze, and Backup procedures. The impact on the user is:

- All users of that post office will be closed out of cc:Mail.
- No exchange of messages will occur between LAN post offices.
- Process will take approximately 1 hour for each 150 MB of data on the post office (i.e., the larger the post office, the longer the procedures will take to complete).

8.1.1.1 CNO-Hub Checkstat/Reclaim

An automatic checkstat/reclaim is commenced on the CNO-Hub of the e-mail system. The impact on the user is:

- No mail exchange between post offices during the reclaim process.
- No dial-in service for remote users.

8.1.1.2 CC:Mail Bulletin Board (AMHS) Cleanup

An automatic cleanup of the cc:Mail Bulletin Boards is started. There is no impact to the user during this process. The cleanup deletes obsolete messages from the boards in accordance with established policies.

8.1.1.3 Total Re-Synchronization of the E-mail Environment

This maintenance will be completed monthly. Any e-mail accounts added to the local post offices without CRC coordination will be deleted.

8.1.1.4 Shutdown of LAN Router Gateways

LAN Router Gateways are automatically shutdown to facilitate other ongoing maintenance. There is no e-mail exchange between the post offices, while router gateways are shutdown.

8.1.2 LAN Server Backups

LAN Servers files are automatically backed up every evening. The process is run in sequence following completion of Mail maintenance procedures. There is a full server backup one day a week, and an incremental backup on other days. Total time to complete the backup for each server is approximately 4-5 hours. There is no operational impact on LAN users during server backups, but any open files will not be backed up. It is important to note that files that are opened are not backed up. It is important to log off after every workday.

8.1.3 Hewlett Packard Database Servers

There are several databases that currently reside on Hewlett Packard Servers. WINPAT is the largest such application. An automated procedure initiates an ORACLE export (special format) of database to an external file. It takes approximately 30 minutes to complete the process.

A backup of system database files occurs nightly. The impact on the users is:

- Database shut down; all user access terminated.
- Database reactivated as soon as backup is complete.

8.1.4 LAN Server Hard Disk Space Management

LAN users have the option of saving data files to workstations, or the directories on the network servers that they have write privileges on (typically “H” - Home Drive, and “T” or “O” Work Group Share Drive). Users are encouraged to save data files to network servers since they are backed up on a nightly basis while workstations are not. There is, however, a finite limit on available disk space on network servers. Users need to take responsibility to delete those files which are no longer current and/or required. The following policies and procedures are intended to guide the users and LAN Administrators in the management of available hard disk space:

- Users have an unlimited amount of data on their “H” drive - home directory.
- When total disk space utilization reaches 80% on a LAN server, the administrator will send warning messages to the ADPSSO’s directing them to work with their users to delete unneeded files. Files that users delete include those on home directories, shared directories that they have write access to, and e-mail mailboxes, folders, and archives. An alternative to deleting files is for the user to archive files to diskette.

- When total disk space utilization reaches 90% on a LAN server, the LAN Administrator will begin deleting files without warning to the users based upon file date/size/location. Games and home software like Quicken will be deleted at any time regardless of server drive space.

SECTION IX REMOTE DIAL-IN POLICIES & PROCEDURES

9.1 Remote Functions Supported

The same basic functions granted to DNHN users on-site are granted on a remote dial-in basis to those users who require that capability. Remote use of DNHN resources is for official Government business only. Remote access to DNHN resources protected by firewalls operated by commercial Internet Service Providers (ISP) is not authorized or supported. Current risks associated with allowing ISP access to the network behind the firewall creates an unacceptable risk to the security posture of the DNHN.

9.2 Establishing an Account

To access the DNHN via remote dial-in, a user must first request a Radius Account. This is done by submitting a remote access request form (Reference: The DNHN Remote Dial-In Policy which is available on DON INPO's web page), via the user's supervisor, to the appropriate DNHN requirements officer (Gary Wyckoff, Director AAUSN ADP, 695-8854, and Barney Thomson, N804J, 695-5038). The requirements officers determine priorities for the installation of remote access software and future distribution of DON INPO laptops.

APPENDIX A: DNHN QUICK START GUIDE

1.0 Getting Started On Your PC

1.1 Powering-on the Workstation

If workstation power is off:

1. Turn on power to computer.
 - a. Plug power cords into the supplied power strip (if required).
 - b. Plug the power strip into the wall outlet (if required).
 - c. Turn the power strip switch on (if required).
 - d. Turn the computer and monitor power switch to the ON position (if required).
2. Allow the memory test to run or press the <ESC> key to skip the test.

The DoD warning screen is displayed. Ensure you are familiar with the DoD warning anywhere on its window.

2.0 Unclassified Network

2.1 Quick Start

To boot your workstation:

Press the space bar on the keyboard..

Turn on the monitor (far right button).

If the system fails to boot: Follow procedures listed in section 1.1.

2.1.1 Logging On

When you boot the machine you will be presented with the screen at the right.

1 . Select "Username" and type your Login ID. (last nameFIMI; Where FI=first inital and MI=middle initial).

2 . Hit <tab> to move the cursor to the "Password" box and type in your password. **Use lower case letters only.**

* The "Domain" box should contain "DoNHQ". If not, <tab> to that field and enter it.

Enter Network Password

Enter your network password for Microsoft Networking.

User name: hudsonle

Password: [masked]

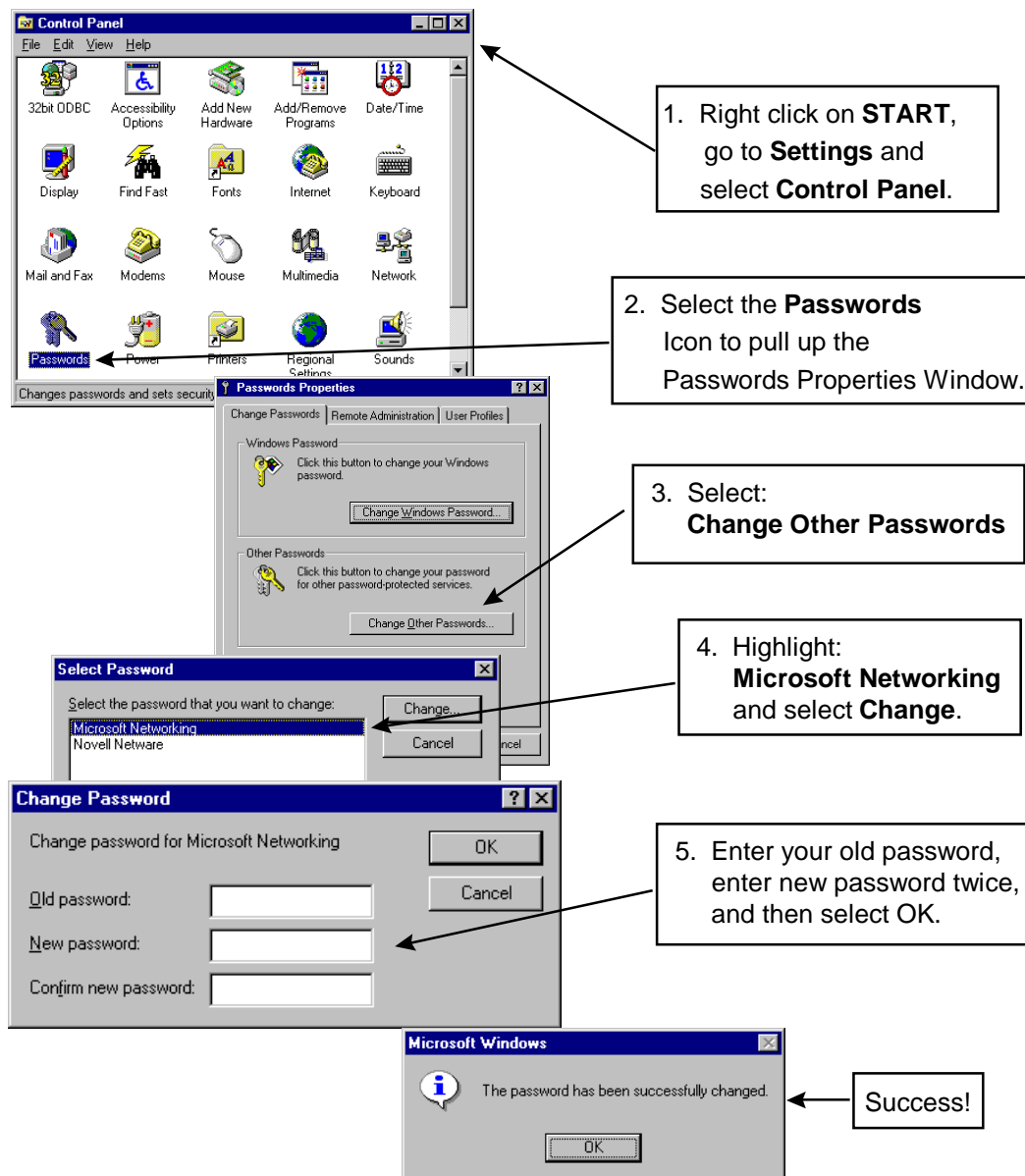
Domain: DoNHQ

OK

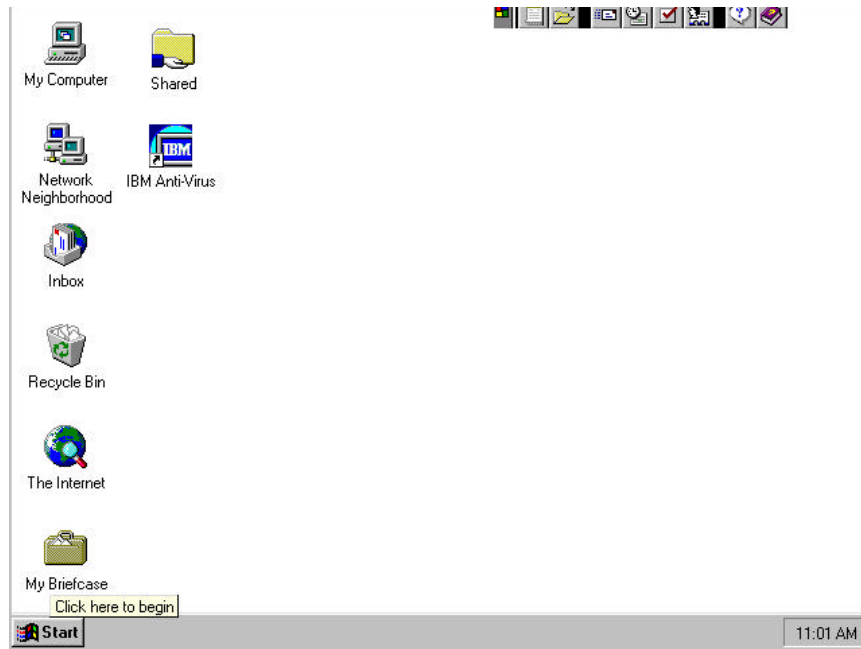
Cancel








3. Select the "OK" button and you will be verified on the network and logged in.




2.1.2 Changing Passwords



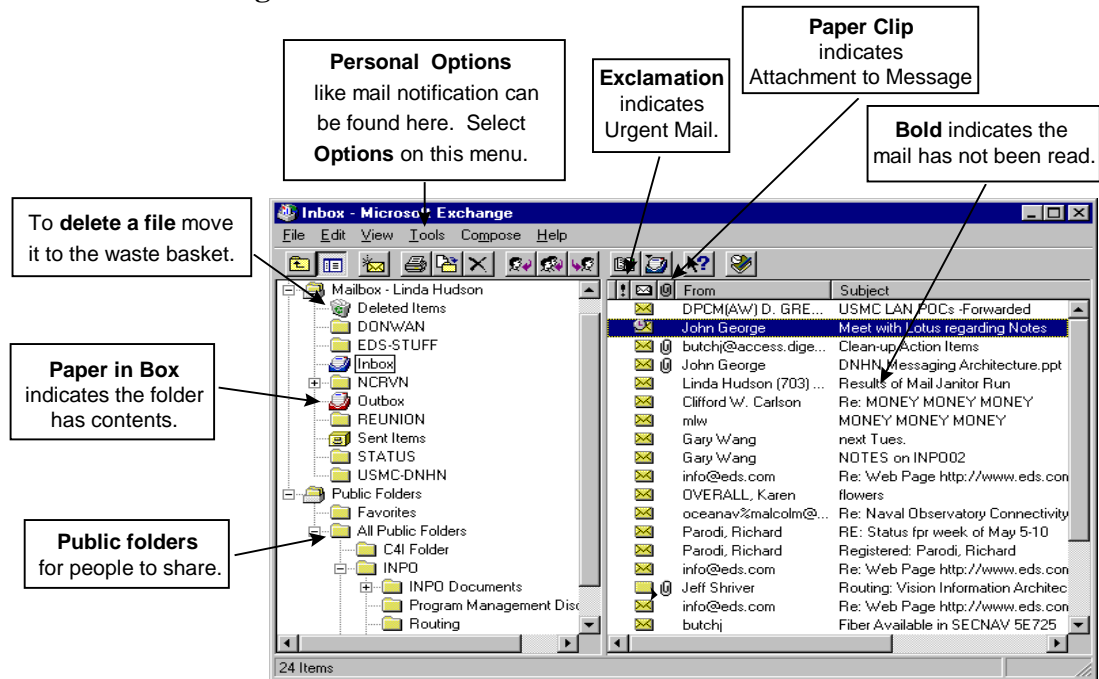
2.1.3 The Desktop



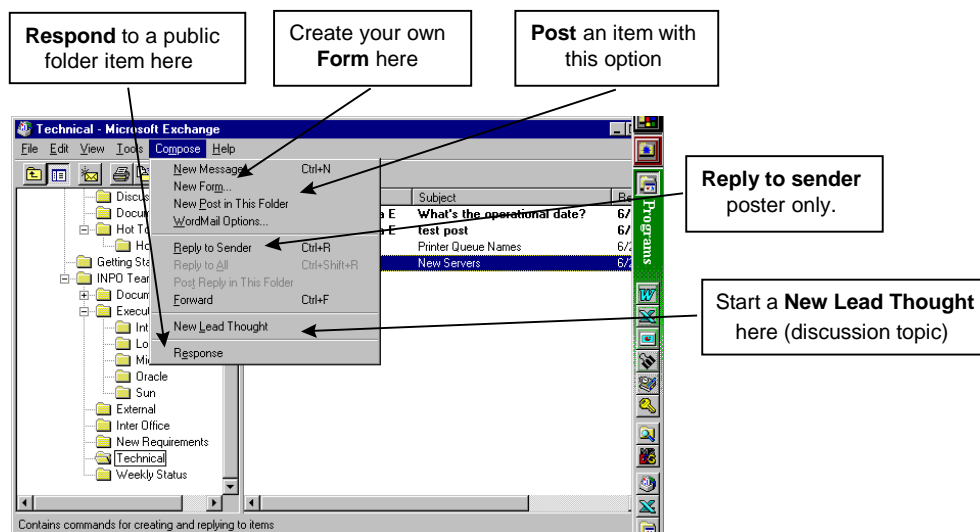
 My Computer	<ul style="list-style-type: none"> • My Computer. Double Click this Icon or Right Click and select Open and a window will display what resources are directly available to your computer. <ul style="list-style-type: none"> – Local drives <ul style="list-style-type: none"> – A: Your 3 ½ “ diskette drive. The new computers have only one floppy drive. – C: Your internal hard disk drive. (Data files stored here are not backed up. – D: CD-ROM drive. – Network drives. <ul style="list-style-type: none"> – G: Global directory that provides access to all users on the DNHN. Folders are provided for major organizational groupings of users. – H: Home directory. This is a private directory for your files only. Files are backed up here every night for safe keeping. Only you have access to this directory. – O: Application directory. This is provided for application updates, patches, etc. Your applications are installed locally on your C: dirve. – System Folders (Control Panel and Printers)
 Network Neighborhood	<ul style="list-style-type: none"> • DoNHQ Network. Double Click this Icon or Right Click and select Open and a window will open displaying other network shares that you can connect to if a shared privilege has been granted to you.
 Inbox	<ul style="list-style-type: none"> • Inbox. Double Click this Icon or Right Click and select Open and you will be connected to E-mail (internal, external and Internet) and scheduling
 Recycle Bin  Recycle Bin	<ul style="list-style-type: none"> • Recycle Bin. Contains files you have deleted. Double Click or Right Click and select Open to list the files that have been deleted. Until the recycle bin is emptied, you can retrieve deleted files. After the bin has been emptied, the files are purged (deleted) from the drive upon which they resided.
 The Internet	<ul style="list-style-type: none"> • The Internet. Double Click or Right Click and select Open to begin “surfing” the net. Defaults to the Navy.Mil homepage.
 My Briefcase	<ul style="list-style-type: none"> • My Briefcase. This is a transfer utility that allows for the transfer of files to/from a laptop computer attached to your local computer or

	<ul style="list-style-type: none"> • Tool Bars. Contains icons for most applications on this machine. There are 6 toolbars available. The standard default is the Program toolbar. Additional toolbars can be added or the toolbar can be customized by clicking the right mouse button over a space in the toolbar.
	<ul style="list-style-type: none"> • Start Button. If you pull the arrow cursor to the bottom of the screen with the mouse, the Start button and Windows 95 menu appears. A left click on the button starts a system of menus that are used to launch applications, files or folders. A right click of the mouse provides a pop up menu that allows the operator to open or find a file.
	<ul style="list-style-type: none"> • Explorer (Windows 95's new File Manager). After a right click of the mouse over the Start button, select Explorer to search the resources available to you.

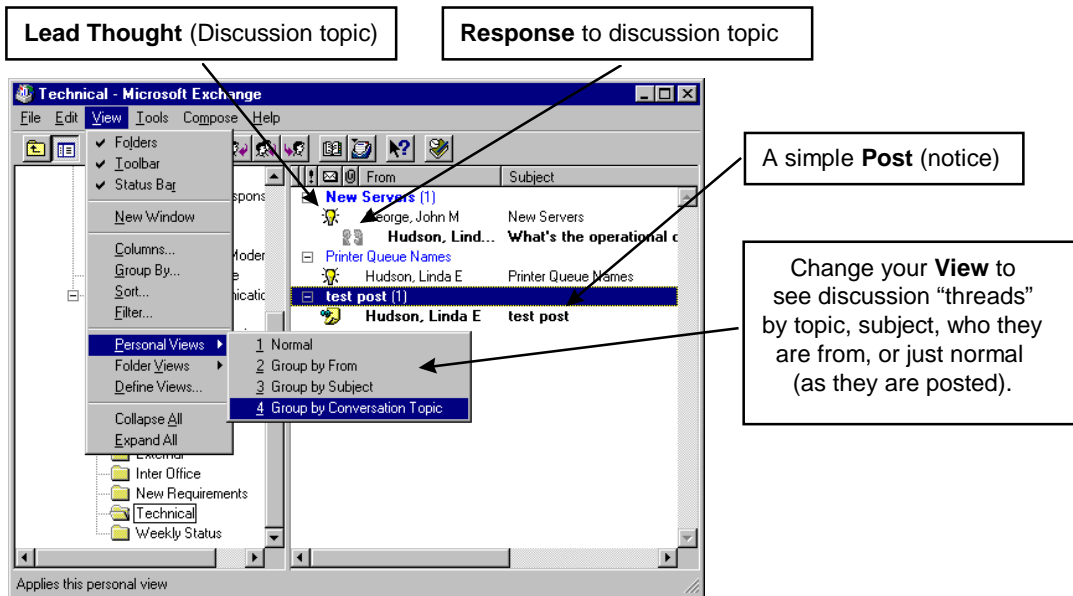
2.1.4 Microsoft Exchange



2.1.5 Compose your thoughts:



2.1.6 Change Point of View



2.1.7 Schedule +

2.1.7.1 Looking at other calendars:

When you launch **Schedule+** you are presented with this screen.

To look at another's schedule choose **File** then **Open** and then **Other's Appointment Book**.

Select a name from the list by typing in the last name or scrolling through the list. Highlight the name and select **OK**.

If they have granted you access, you will see their schedule.

If that user has not granted you access, you will be denied with the message below.

The screenshots illustrate the steps to view another user's calendar in Microsoft Schedule+. The first window shows the 'File' menu with 'Open' selected. The second window shows the 'Open' submenu with 'Other's Appointment Book...' selected. The third window shows the 'Open Other's Appt. Book' dialog box with a list of users, including 'Bailey, Stuart W'. The fourth window shows the 'Bailey, Stuart W - Microsoft Schedule+' window displaying his calendar. The fifth window shows an error message: 'The schedule file could not be opened. Access is denied.'

2.1.7.2 Giving others access to your calendar:

1. To give others access to your calendar, select **Set Access Permissions...**

Select **Add** to locate a new user to grant permission to (the default is none).

Predefined Permissions:

None: No permission to user.

Read: Allows the selected user read-only access, except for items marked private.

Create: Allows the selected user to read existing items and create new items, except for items marked private.

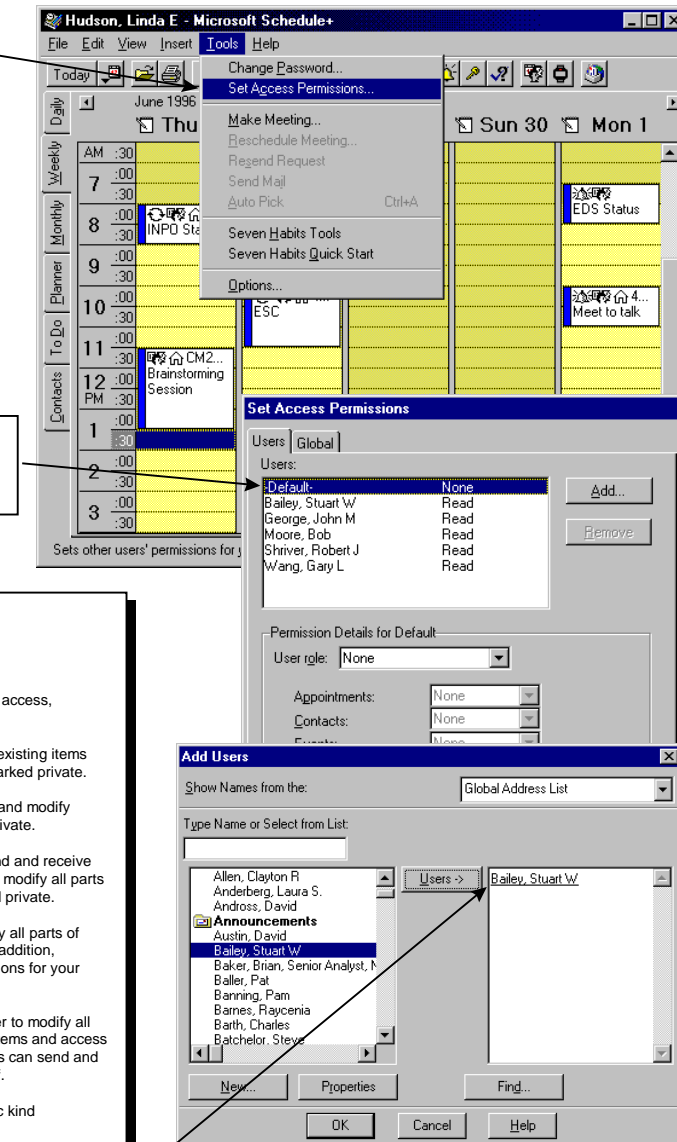
Modify: Allows the selected user to read and modify existing items, except for items marked private.

Delegate: Allows the selected user to send and receive messages on your behalf. A delegate can modify all parts of your schedule, except for items marked private.

Owner: Allows the selected user to modify all parts of your schedule, including private items. In addition, Owners can change user access permissions for your schedule.

Delegate Owner: Allows the selected user to modify all parts of your schedule, including private items and access permissions. In addition, Delegate Owners can send and receive meeting messages on your behalf.

Custom: Give the selected user a specific kind of access for a specific kind of item.



Select a user to add and click **OK**.


2.1.8 Internet Explorer

Customize your Internet Explorer here by choosing **Options** on this menu.


Search the internet for URL's by choosing **Search the Internet** on this menu.

Save your favorite URL's here by choosing **Add to Favorites** under this menu.

The Universal Remote Locator (URL). Every internet site has a URL.



Start your collection of favorite URL's by adding them here.



2.1.9 Logging Off

2.1.9.1 Changing Users During the Workday

It is recommended that all users apply these procedures for logging off the LAN.

- Click Start Button.
- Click Shut Down.
- Click radio button labeled “Close all programs and log on as a different user?”
- This will display the Enter Network Password window.
- New user logs on as indicated above.

2.1.9.2 Logging Off End of Day

- Click the Start Button.
- Click Shut Down.
- Click radio button labeled “Shut down the computer?”
- Turn off the monitor (Windows 95 will power off the computer).

2.2 Applications

DNHN provides the Microsoft Office suite of products, the Microsoft Internet Explorer, and Microsoft Exchange which includes a calendaring application called “Schedule +”. Version numbers and additional information are provided below:

- **Microsoft Word V6.0/7.0.** A new version which is backward compatible with the existing MS Word you have on the classified LAN.
- **Microsoft Excel V7.0.** A new version which is not backward compatible with the Excel 6.0 version currently on the classified LAN. You can save a version 7.0 document as a version 6.0 if you need to work on a file on a computer with version 6.0 loaded.
- **Microsoft PowerPoint V7.0.** A new version which is not backward compatible with version 4.0 (the earlier version). You can, however, save the file as a version 4.0 file (use Save As option), if you need to read it with the earlier version.
- **Microsoft Access - V7.0.** A new version which is backward compatible with the previous version.
- **Microsoft Exchange V4.0.** A completely new mail system with greatly enhanced capabilities. With this new mail system we are positioning ourselves for the upcoming Defense Messaging System (DMS). You, as the user, will find it easy to use and very intuitive. It provides the following capabilities:
 - Public Folders: a place to put public mail for all to see.
 - Personal Folders: for your own personal mail storage.
 - Integrated Calendaring: to schedule meetings and much more.
 - Bulletin Board Service: for public announcements, postings, and discussion threads.
 - Directory Services: to look up addresses.
- **Microsoft Schedule + V7.0.** The user interface is very user friendly and is integrated with Microsoft Exchange allowing meeting notices to pass through e-mail to not only those on the system but anyone in Personal Address or Global Address Books added as recipients. Schedule + users will automatically see meeting notices in respective calendars.

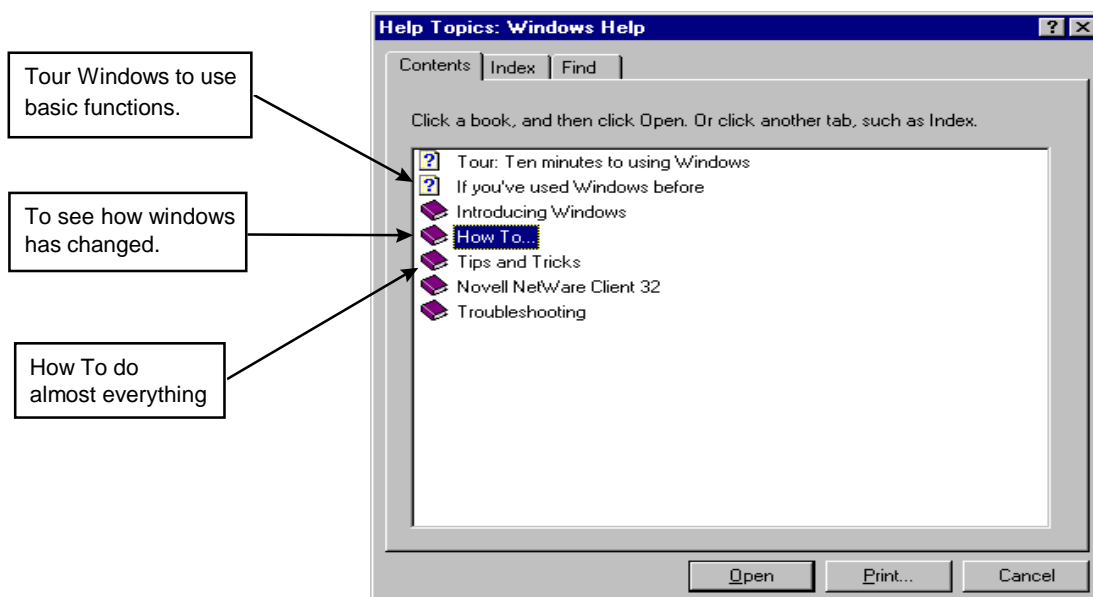
- **Microsoft Internet Explorer V3.0** Upgrade to 4.0 planned.
- **McAfee Anti-Virus Protection**

2.3 How do I.....

Customize the Microsoft Office Button Bar:

Right click on the blank space between icons on the button bar (not on an icon) and choose Customize.

2.3.1 Find HELP:



2.3.2 Activate Windows 3.11 Program Manager:

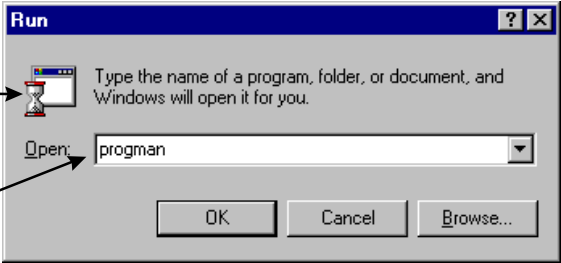
If Windows 95 becomes too confusing, you can run the Windows 3.11 Program Manager until you become familiar with it.

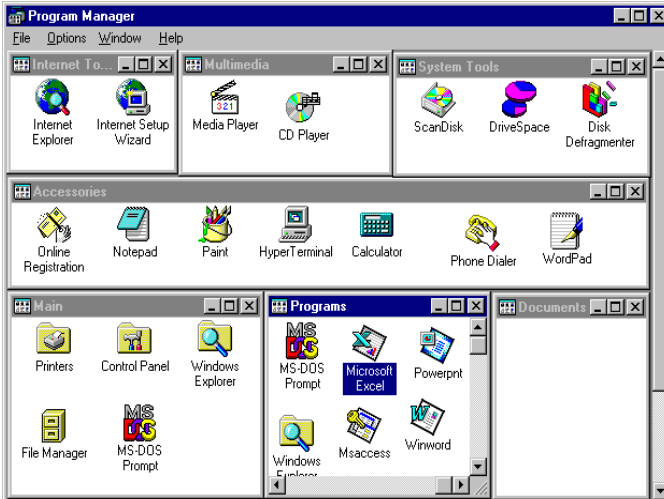
To run Program Manager, perform the following steps:

1. Left click on the **START** button and select **Run**. You will be presented with the **Run** window picture at right.

2. Type "progman" in the "Open" window and select the OK button.

3. Program Manager appears





3.0 DNHN Classified LAN

Once workstation is powered:

1. Windows for Workgroups (WFW) Version 3.11 is the standard desktop on the DNHN *CLASSIFIED* workstations. The Logon dialog box is automatically opened for the user after the desktop is set up. The user should enter the following information in the Logon dialog box:

Logon Name (your assigned N-Code)

Password

Domain

2. Click on the OK icon. The user's log in script will be run (validating password and connecting user to his/her authorized network resources).
3. Upon completion of the log-in process, the Windows for Workgroups.

Note: New users should enter the ADPSSO assigned password. Select an individualized password during the initial LAN session (see "Changing Passwords" section below). Users normally only have to enter the password. Default entries are automatically entered for the Logon Name (individual who normally uses the workstation) and the Domain. Any default entry can be overwritten by the user. DNHN users can logon to the network at any workstation connected to the LAN and still have access to their home directory ("H" drive), cc:Mail, and Lotus Organizer files (Class LAN).

3.1 Passwords

Access to the CLASS LAN and it's files are supported by at least two UserIDs, one for the LAN file server and the other for cc:Mail. The LAN UserID is the user's N-code (e.g., N651L1). The cc:Mail UserID, however, also identifies the user's organization (e.g., CNO-N651L1). The organization is included in the cc:Mail UserID to identify the user on Wide Area Networks (WAN).

3 .1.1 How to Change the LAN Password:

1. Double-click on the Control Panel Icon in the Main Group.
2. Double-click on the Network Icon.
3. Click Startup in the Options box.
4. Click Set Password button.

5. Enter your original password in the box - Old Password and then <tab>.
6. Enter your new password in the box - New Password and then <tab>.
7. Re-enter your password in the box - Confirm New Password.
8. Click OK to exit the Change Domain Password Window (the dialog box will confirm the password change).
9. Click OK to exit the Startup Settings Window.
10. Click OK to exit the Microsoft Windows Network Window.
11. Close the Control Panel Window.

3.1.2 How to Change the cc:Mail Password:

1. Double-click on the cc:Mail icon and log into cc:Mail.
2. Select - Tools.
3. Select - User Set-Up.
4. Click on the Password Button.
5. Select - Old Password.
6. Type in your old password <TAB>.
7. Enter New Password <TAB>.
8. Confirm new password by entering it again in the New Password Again box.
9. Click OK to exit User Setup Window and return to cc:Mail.

3.1.3 What if I forget my password?

The CRC can reset the password for user LAN, cc:Mail, or Lotus Organizer accounts (usually occurs when user is locked out of his/her account(s) due to expired or forgotten password). The CRC will only accept requests from the user's ISSO, or ISC representative. The only exceptions to this policy will be for O-7's and above. In those cases, the CRC will send a representative to the user's office to accomplish the reset.

3.2 DNHN Classified Applications

The following groups and applications are available on the standard DNHN CLASSIFIED Windows for Workgroup Desktops:



3.2.1 Network Applications (Shared) Group

Microsoft Word 6.0c
Microsoft Excel 5.0c
Microsoft PowerPoint 4.0c
Lotus Organizer 2.1
MTF Editor 3.5
Microsoft PowerPoint Viewer 4.0
Lotus cc:Mail 2.21
Lotus cc:Mail Notify 2.0
Microsoft Office 4.3
McAfee Anti-Virus 2.1
WINPAT 3.34

3.2.2 Global Applications (Shared) Group

DNHN User's Guide OPNAV Locator
Defense Auth/Appn Bills
Early Bird

Global Apps Info
OPNAV Bulletin
DPVS 4.00
SNDL
OPNAV Administrative Manual
CD-ROM Library
Secure Mail Guard User's Guide
OPNAV/SECNAV Space Moves and Renovation

3.2.3 Organizational Apps (Shared) Group

This group contains applications that are required by an entire N-Code organization, but which are not in the Network or Global Applications Groups.

3.2.4 Local Applications Group

This group contains any DNHN approved applications that the user requires, but which aren't in any of the other workstation groups. Any application the user installs (i.e., to his/her workstation) should have the associated icon(s) placed in the Local Applications Group.

3.2.5 Accessories Group

The standard accessory programs that are part of MS Windows for Workgroups 3.11 such as Paintbrush, Notepad, Card File, Calculator, etc.

3.2.6 Main Group

The standard utility programs that are part of MS Windows for Workgroups 3.11 such as File Manager, Print Manager, Control Panel, MS-Dos Editor, MS-Dos, and the network log-on/log-off icon.

3.2.7 StartUp Group

Contains those programs that are automatically started when the user boots a computer. Users can copy any application into this group by highlighting the icon, holding the CTRL key down, placing the mouse pointer on the desired icon, pressing the left mouse key down, and then dragging the duplicated application icon to the StartUp Group.

3.2.8 Microsoft Office Manager

Provides users with a single click access to the most commonly used network applications. Miniature icons can be set-up to be always visible and can be placed on top of all current user programs. It can be customized (any application icon can be added or deleted) by the user to suit his/her preference.

3.2.9 Lotus Organizer V2.1

Lotus Organizer is the standard DNHN Classified Personal Information Manager (PIM) application. It uses the metaphor of a notebook with sections for appointments, lists of things to do, names and addresses, anniversaries, yearly plans, and notes. The sections can be customized by the user. Sections in other people's files can be included in personal files for viewing and editing. Full group and resource scheduling is enabled for this application. Each DNHN user has his own Organizer file. The files for your N-Code's users are stored in a global LAN share. This allows all authorized DNHN users to interact with each other's files. The naming convention is the user's N-code (e.g. CNO-N651L1) to ensure that two files are not named the same. The user **MUST NOT** change the name or location of the saved file, or the capability to do Group/Resource scheduling with their Lotus Organizer file will be lost. The N-Code you logged on to the LAN with is the Organizer file that is automatically opened when you launch Lotus Organizer.

3.2.9.1 Passwords for Lotus Organizer:

The logon screen for Lotus Organizer requires a password. You should enter your cc:Mail password. Lotus Organizer uses that password to validate you as a user and to determine what level of permission you should be granted for files you attempt to open. You can also create a separate Lotus Organizer password. This, however, will only be used if you aren't validated by an e-mail system (i.e., cc:Mail).

3.2.9.2 Access Control Lists (ACL):

Each Lotus Organizer 2.1 file has an Access Control List (ACL) associated with it. That ACL determines who has privileges to that file, and what level of privileges they have. Only LAN Administrators and file owners can change a file's ACL. Initially, the only entries in an ACL are the owner and a *DEFAULT* (i.e., everyone else). Other individuals can be added to an ACL with associated file permissions. There are six levels of permissions:

- | | |
|-------------|---|
| (1) Owner | Gives full access rights to your file, including read, assistant, customization, and free time access. Owners can access entries set to confidential and can also set the access level for users. |
| (2) Trustee | Gives read, assistant, and free time access to your file. Trustees can also customize your file. Trustees cannot view or change entries that are confidential. |

- (3) Assistant Gives read, write, and free time access to your file. Assistants can also schedule and respond to meetings in your file and change preferences. Assistants cannot view or change confidential entries.
- (4) Reader Gives free time access and also read access to entries in your file that aren't confidential.
- (5) Free Time Gives read access only to the free time in your calendar during group scheduling.
- (6) None Give no access to your file.

3.2.9.3 Including Sections of Files:

Sections of other files can be included in individual Lotus Organizer files. Privileges on that information are determined by that file's ACL. The file you are including the section from MUST be specified as CNO-Nxxxxx and not as the name or the N-code (i.e., CNO-N651L1, not O'Connor or N651L1) or you will not have the full group scheduling capability in that included section.

3.2.9.4 Group Scheduling:

Invitations can be sent from your Lotus Organizer file to other Lotus Organizer account holders to attend a meeting. The invitation can be sent (with an attachment if desired) to an individual or to a group of people (using a pre-defined cc:Mail mailing list). You must open the file with the primary cc:Mail identification (e.g., CNO-N651L1) to have the Group Scheduling capability in Lotus Organizer.

3.2.9.5 Room and Resource Scheduling:

Conference rooms and resources (e.g., laptop computers, overhead projection devices) can be reserved by Lotus Organizer file. Rooms and resources are set up to automatically accept and schedule an invitation if they aren't already booked for the requested time. In order for the room or resource to be available for Lotus Organizer scheduling, the owner of that room or resource must put a request in to the DNHN Customer Response Center (CRC) at "HELP" or 697-6464. The rooms that are available for scheduling can be identified by the "RM-" prefix on their name (e.g., RM-5A726-N6). The N-Code at the end of the room name identifies the owner of that room. The resources that are available for scheduling can be identified by the "RE-" prefix on their name.

3.2.10 Modification of Icons in Shared Groups

Users should not make changes (e.g., insert new application icons) to any of the shared groups (Global Apps, Network Applications, and Organizational Apps). Changes that are made to those groups will be overwritten and lost when a LAN global update is performed (new program added to group, or application update). If a user desires to create or modify an icon (e.g., load an application on their local workstation hard drive), the icon should be placed in the *Local Group*.

3.2.11 Path Assignments

There are numerous logical and physical disk drives available for LAN use. The following breakdown will explain how software, data files, and devices are stored on the LAN and which drives are available for your use:

3.2.11.1 Local Drives (on User Workstations)

- A, B: Either 5 1/4" or 3 1/2 diskette drives.
- C: Internal Hard disk drive on your workstation. Data files stored here are not accessible on the network, and must be backed up by the user.

3.2.11.2 Network Drives (on LAN Servers)

- G. Global Directory that provides access to the DNHN global services. All DNHN users that have a direct connection (all except N00K and N42 Crystal City) can read files in this drive, but write/edit permissions limited CRC (697-6464).
- H: Home directory for each user's work files. Files stored in this directory are
 - cc:Mail: Used for archiving or storing messages.
 - MSOFFICE: Default working directories for the MS applications.
 - EXCEL: User files and default directory for Excel 5.0.
 - XLSTART: Start-up template and macro directory for Excel 5.0.
 - ORG2: Contains user customized print layouts and archived files for Organizer 2.1.
 - POWERPNT: User files and default directory.
 - SETUP: Contains network configuration information for MS Office.

WINWORD: User files and default directory for Word 6.0.

STARTUP: StartUp user macros for MS Word.

TEMPLATE: Contains user template files for MS Word .

MTFMSGs: User files and default directory for MTF Editor 3.5.

OLDHOME: Any H Drive files that user had prior to block I.
(note: These should be archived or deleted)

WPWIN: User files and default directory for WordPerfect 5.2

I: Immediate office share (working group) within the overall N-Code (Users will be able to access the files in any sub-directory that they have privileges to). Requests to increase access privileges should be addressed to the specific N-Code's ADPSSO.

M: Network applications. (Read-only access)

O: Organizational share directory for an entire N-code. All users in the N Code have read, write, and delete permission for all files and subdirectories.

P: CC-Mail user files.

R-Y: Temporary LAN connections made when user selects one of the applications in the Global CD-ROM library. Drive will be disconnected once user exits his/her WFW desktop.

Note: *Windows For Workgroups (WFW) gives users the capability to connect to other network resources (e.g., another user's hard disk - if designated as a shared resource). The logical drive letter will default to the next available letter. The user can override the selection and can decide whether to automatically connect to that resource during future network logons. Those connections will only be made when logging on to the network from the workstation the request was initially made at.*

3.2.12 Printer Ports

LPT1: Reserved for local printers

LPT2: Reserved for network printers

LPT3: Reserved for network printers

Note: *User's are automatically connected to a default network printer upon LAN logon. The default network printer can be identified by the user launching the Print Manager icon in the Main Group.*

User's can use the print manager to temporarily connect to any other printer on the DNHN. Any temporary connection will be overwritten on the next LAN login. If a user desires a permanent change in their default network printer, they should contact the DNHN Customer Response Center - CRC (202) 433-0600

3.3 Running Applications

This section provides basic information on working with applications running on your MS Windows For Workgroups workstation. Detailed information should be obtained by attending one of the software training classes at the DNHN Computer Training Center (5E562, 693-8100), and reviewing the MS Windows For Workgroups User's Guide that is stored near each workstation.

As you work with MS Windows for Workgroups, there are a few basic terms you need to become familiar with. You do your work in rectangular areas of the screen called *windows*. Windows appear on a background called the *desktop*. The applications you work with (such as your word-processing or spreadsheet applications) are represented in Windows by small graphical symbols called *icons*.

You can start an application by double-clicking its program-item icon with the left mouse button. When you double-click ("choose") the icon, the application is opened and appears in an application window, ready for you to use. Each application window provides a *menu bar* which lists available application *commands* in a *menu* format. You can simultaneously open multiple windows. The maximum number depends on your workstation's resources. The active window is generally the window in the foreground. To make another window active you just need to use the mouse to click anywhere on its window.

As you work with Windows for Workgroups, you may want to temporarily put aside an application but keep it running and easily available for later use. You can avoid clutter on your screen if you reduce the application window to an icon by clicking its Minimize button (see the Microsoft Windows User's Guide for more details.) The icon stays on the Windows desktop until you need to use the application again. Users should limit the number of applications they minimize, or the performance of the active application will suffer.

When you finish using an application, you will want to close it to free your workstation's memory for other tasks. There are several ways of accomplishing this which are described in the MS Windows User's Guide. To run an application, do the following:

- 1) Point the mouse cursor to the application icon.
- 2) Double Click the left button of the mouse to open the application. An hourglass is displayed while your workstation is working to remind you to wait until the system can complete your requested task..
- 3) Work with the application once opened (minimizing and maximizing application windows as required).

- 4) Close all application windows prior to logging off the LAN.

3.3.1 Saving Files On The DNHN

3.3.1.1 Overview

LAN users have numerous options on where they save data files. Some of those choices include saving to their Home directory on the LAN, a shared directory on the LAN, their workstation's hard drive, or floppy diskettes. There is, however, a finite amount of server hard disk space on the LAN. Users must comply with LAN management procedures and actively archive and delete their old and obsolete files.

3.3.1.2 CC:Mail

CC:Mail files and messages are of particular concern due to the number and size of those files and attachments. The operational requirement for rapid communication between the DNHN staffs and with outside agencies has made electronic messaging (via cc:Mail) a critical application on the DNHN. Daily maintenance (including file backups) is essential to ensuring rapid system response and high reliability. There is a limited amount of storage space on the network servers. Lack of available server Post Office space prohibits the completion of the daily mail maintenance. You as a LAN user have a direct impact on the reliability of cc:Mail! It is essential that you assist the LAN support staff by properly managing your cc:Mail files. The following info gives guidance on different cc:Mail file management options:

3.3.1.3 Trash

Once a message is read, immediately place it in the trash icon if you no longer need it. Leaving unneeded messages in your mail inbox is a waste of valuable server post office space. At least once a day (e.g., close of business) click on the empty trash icon to free up post office space.

3.3.1.4 Message Logs

The default user setup saves all outgoing messages in a Message Log. The Message Log is a folder also, which means its messages takes up space in the postoffice. Users should periodically review their Message Log and delete those messages that are no longer required.

3.3.1.5 Saving Messages outside of cc:Mail

If users need to keep a message and/or its attachment(s) as a reference, save messages or attachments to floppy disk (A or B), workstation hard drive (C), or Home Directory (H). Users can then access these files from applications other than cc:Mail, liberating scarce disk space in the Post Office. These are the preferred destinations for saving cc:Mail messages, and attachments (i.e.

PowerPoint, Excel, MS-Word, etc.). Saving files to the “H” drive will allow the user to gain access from the files at any OPNAV LAN workstation.

3.3.2 ARCHIVES vs. Folders

CC:Mail provides two convenient areas in which messages can be saved - Folders and ARCHIVES. Folders and Archives allow assigning a name to files and organizing according to needs - by topic, by month received, by originator, etc. Messages in a folder can be deleted by simply "dragging" messages to TRASH. Archive entries cannot be deleted individually. You must copy a message out of an archive (to a folder or inbox) or delete the entire archive. An important difference between folders and archives is the impact on the post office. Messages retained in Folders continue to take up space within the post office. Moving a message from your INBOX to a folder does NOT remove it from the post office. Moving it to an Archive does! This is important because it reduces the size of the post office. For those messages you need to save for future cc:Mail reference use your folders as a "short term" repository for messages (60 days or less), and use the archive for those messages that need to be retained for longer periods of time. Attachments such as POWERPOINT graphics can take up a considerable amount of space in the post office. Delete attachments (if not needed) prior to saving the message(s) in archives or folders.

3.3.3 Logging Off DNHN

To maintain security over the DNHN Classified (SECRET HIGH) LAN, you are required to log-off the LAN when your workstation will be left unattended for greater than 30 minutes.

3.3.3.1 To Log-Off the LAN do the following:

- Double Click the Log On/Off Icon in the Main Group.
- Click the Yes button in the Windows For Workgroups window.
- Click OK in the Log On/Off Window.

APPENDIX B: FREQUENTLY ASKED QUESTIONS

The following are some commonly asked questions by LAN users, along with the answers that usually solve the problem:

Q: Why did I get a message that I couldn't connect to an application when I attempted to start it?

A: Majority of user applications are located on the LAN servers. Users can only gain access to those programs if they have a good network connection. Users should first verify that they are connected to the network by clicking on the Log On/Off icon in the Main Group. If that doesn't fix the problem, exit Windows for Workgroups and then re-enter. The user scripts will be re-run which should establish proper connections for the user to the LAN.

Q: How do I save my Windows for Workgroups desktop setting without selecting SAVE SETTINGS ON EXIT?

A: Selecting SAVE SETTINGS AT EXIT will save the appearance of your WFW desktop when you exit it. Another option is to hold the SHIFT key down, and select the upper left bar in the WFW Program Manager and then selecting CLOSE in the drop down menu that appears. The WFW desktop will then be saved but you will not exit WFW.

Q: How do I customize the Microsoft Office Button Bar?

A:

1. First check the properties of the application you want to add by highlighting it in the Program manager
2. Single Click File.
3. Single Click Properties....
4. Make note of application's Description, Command Line and Working Directory.
5. Hit <ESC> .
6. Single Click the button on the far right of the MS bar (the Microsoft Office Button)
7. Single Click Customize....
8. Single Click Toolbar.

9. Single Click the Button Add....
10. Type in the Description that you made note of in the properties before.
11. Hit <tab>.
12. Type in the Command Line that you made note of before.
13. Hit <tab>.
14. Type in the Working directory that you made note of before.
15. Single Click the OK button.
16. Single Click OK button.

To learn more about the new features in the Microsoft Office Suite (Word, Excel, PowerPoint), select “Examples and Demos” from the Help menu item. Note: You cannot print information that is in a pop-up window.

Q: How do I Activate cc:Mail Notify?

A:

1. Double click the CC:Mail Notify Icon located in the Network Applications Group.
2. Single click Mail.
3. Single click Delete User.
4. Delete all users listed.
5. Single click Mail.
6. Single click Add User.
7. Type your User Name (CNO-User N-Code)
8. Hit <tab>.
9. Type your CC:Mail password.
10. Hit <tab>.
11. Type P:.

12. Single click the OK button

13. Single Click Options

14. Look to see if Keep Password when saved is checked. If it is, hit the ESC key on your keyboard. It isn't, single click that option so the check mark is in the box.

15. Single click Mail

APPENDIX C:
MEMORANDUM OF AGREEMENT FOR USER
ACCESS TO DNHN COMPUTER SYSTEMS

Date:

To: Department of Navy Headquarters Network Information Systems Security Officer

Subj.: MEMORANDUM OF AGREEMENT FOR USER ACCESS TO DNHN COMPUTER SYSTEMS

Ref.: (a) DNHN IS SYSTEM SECURITY PLAN
(b) SECNAVINST 5239.3
(c) User's SOP for DNHN

1. This Memorandum of Agreement (MOA) is required to be signed by each user prior to them being granted access to the DNHN.

2. As a user of the DNHN IS systems, I understand that I am responsible and accountable for following all requirements of reference (a). I am solely responsible for all access and actions carried out under my user identification, and password. I agree to the following conditions:

- a. The requirements of references (a) and (b) will be met prior to access being requested.
- b. The password will be kept confidential and will not be disclosed to anyone, will not be electronically stored, and will be committed to memory.
- c. The password/log-on identification key will not be transferred to anyone else due to reassignment or transfer or termination.
- d. Limit the use of DNHN to official government business.
- e. Computer fraud will not be committed. This includes, but is not limited to:
 - unauthorized input of false records or data into the system.
 - unauthorized use of computer facilities (i.e. theft of computer time) including use of a user name or password other than one's own.
 - unauthorized alteration or destruction of information, files or equipment.
 - introduction of unauthorized systems/software into the DNHN.

- introduction of viruses, worms or any other destructive program into the DNHN.

f. The ADPSSO will be immediately notified of suspected cases of computer fraud.

g. In the event of a compromise of a password, whether suspected or confirmed, the compromise will be immediately reported to the ADP SSO or the CRC and password modified.

h. Do not enter, display or process classified data where visible to unauthorized personnel.

i. Do not circumvent security requirements to obtain unauthorized access.

j. Notify ADP SSO or the CRC in writing when access to the DNHN is no longer required due to reassignment, transfer or termination.

k. Immediately access the DNHN user account after issuance and modify the password.

l. Notify DNHN ADP SSO of changes to system configuration.

m. Software not purchased or licensed by the Department of the Navy will not be installed on the systems without prior written approval.

3. The following information must be provided for access to be granted.

a. User Name: _____
(Rank, DOD Status, Contractor): _____
SSN (Last Four): _____ Phone: _____
Clearance Level: _____

b. Command and Location: _____
Code: _____ Room: _____

4. I certify that the above information is correct to the best of my ability and I will comply with the terms of this agreement. I further certify that I have read and understand reference (c) and will comply with all its requirements and provisions.

Requester Signature and Date

I certify that the security requirements identified in reference (a), have been met and that the security clearance of the requester is correct. I agree to notify the DNHN ISSO immediately of any action taken to revoke or downgrade the requester's security clearance.

ADPSSO Signature and Date

PRIVACY ACT STATEMENT

OPNAVINST 5239.1A authorizes the collection of this information. The only use of this information is by the ISSO and system management personnel to identify authorized users requesting access to DNHN resources.

This form is valid for one year from the date access is granted, it must be renewed annually thereafter. The original will be maintained in the ISSO office for two (2) years for record purposes.

APPENDIX D: LOCAL AREA NETWORK (LAN) SECURITY BRIEFING OUTLINE

This brief is required by the Department of the Navy Headquarters System (DNHN) Information Systems Security Plan. The purpose of the briefing is to familiarize users with their responsibilities when working with the DNHN systems, and to assist in achieving an effective security posture in each organization.

Clearance:

Users must have a security clearance at least to the level of the network's classification.

Need to Know:

The system hardware and software is operated as a need-to-know system. In this mode, the entire system, including all components electronically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity (e.g. SECRET) of the data being processed and/or stored. Even though all users have at least a secret clearance, not all have the same need-to-know. Ensure your E-mail recipients have a need-to-know when sending them messages.

Passwords:

LAN passwords must be at least six (6) characters. They should be difficult to guess, should not be written down, and shall not be shared with another person. Your workstation may be shared, but the user shall have his/her own UserID and Password.

Log-Off:

DO NOT leave your workstation unattended while logged on the LAN. Log off the LAN during those periods to prevent unauthorized users from gaining access to the network resources.

Protect Classified Equipment:

Users are responsible for protection of the classified system's equipment. Do not allow classified equipment to leave your work space(s) without proper authorization from your LAN Administrator or ADPSSO. Releasing equipment without that authorization is a violation of security regulations. **YOU WILL RECEIVE A SECURITY VIOLATION** as a result of failure to comply.

Software:

Only software approved by Department of the Navy Information Networking Program Office (DON INPO) may be utilized on the DNHN systems. This includes software on the user workstations in addition to those on the servers. Virus check all software (using the system's Anti-Virus program) before loading it on the system.

Check-Out:

When you are reassigned, you must check-out with your ADPSSO. The ADPSSO will ensure that your LAN accounts are deleted. DO NOT pass your UserID and password to your billet relief. You will be responsible for any security violation caused by your relief if you don't comply with this requirement. Your relief must acquire their own account.

I certify that I understand and will comply with all items discussed during this briefing on LAN security (particularly regarding Log-Off and Software):

Date_____ Signature_____ Organization_____

APPENDIX E: FILE TRANSFER PROCEDURES FOR COPYING FILES BETWEEN CLASSIFIED AND UNCLASSIFIED LANs

Each office has access to a suite of secure transfer utilities on the CLASS LAN. Each office should create a “Toolbox Floppy” stock of diskettes which have been prepared with the “Flush” utility described below and labeled for exclusive use in copying files back and forth between the CLASS and UNCLAS LANs. It is recommended that this stock be kept in a designated location. The container used to stock the diskettes should have three sections. The first section should be labeled “Flushed” and be reserved for diskettes that have had the FLUSH utility performed on them and have not been used to transfer files thereafter. The second section should be labeled “Used” and be reserved for diskettes that have only been used a few times to transfer files. The third section should be labeled “Needs Flush” and be reserved for diskettes that have been used often to transfer files and that need to have the FLUSH utility performed on them in order to expedite execution of the BUSTER utility.

Floppy disks must have a green “UNCLAS” security label, and a DNHN UNCLASSIFIED DISKETTE INFORMATION LABEL and should be clearly marked as “Toolbox Floppy” to discourage use for other purposes. The “Toolbox Floppy” disks must initially be new disks. They may be used repeatedly for file transfer between the LANs as described above. A disk should be run through FLUSH when BUSTER becomes unwieldy because it is operating on the accumulation of files processed on the disk since the last Flush.

Note: FLUSH wipes files from disks. BUSTER scans for classified files and data.

File Transfer Procedures Between Unclassified to Classified LAN

1. Take a flushed or used floppy from the “Toolbox Floppy” stock of diskettes
2. Ensure that the Write Protect tab on floppy is down/closed.
3. Insert diskette into the UNCLAS PC floppy drive
4. Copy file(s) from the UNCLAS PC to the floppy.
5. Remove diskette from the UNCLAS PC and change the Write Protect tab to up/open position.
6. Insert the diskette into the CLASS PC and copy the file to where it is needed using File Manager or from any other application
7. Return the diskette to the “**Toolbox Floppy**” stock.

4.7.2 File Transfer Procedures Between the Classified and Unclassified LAN

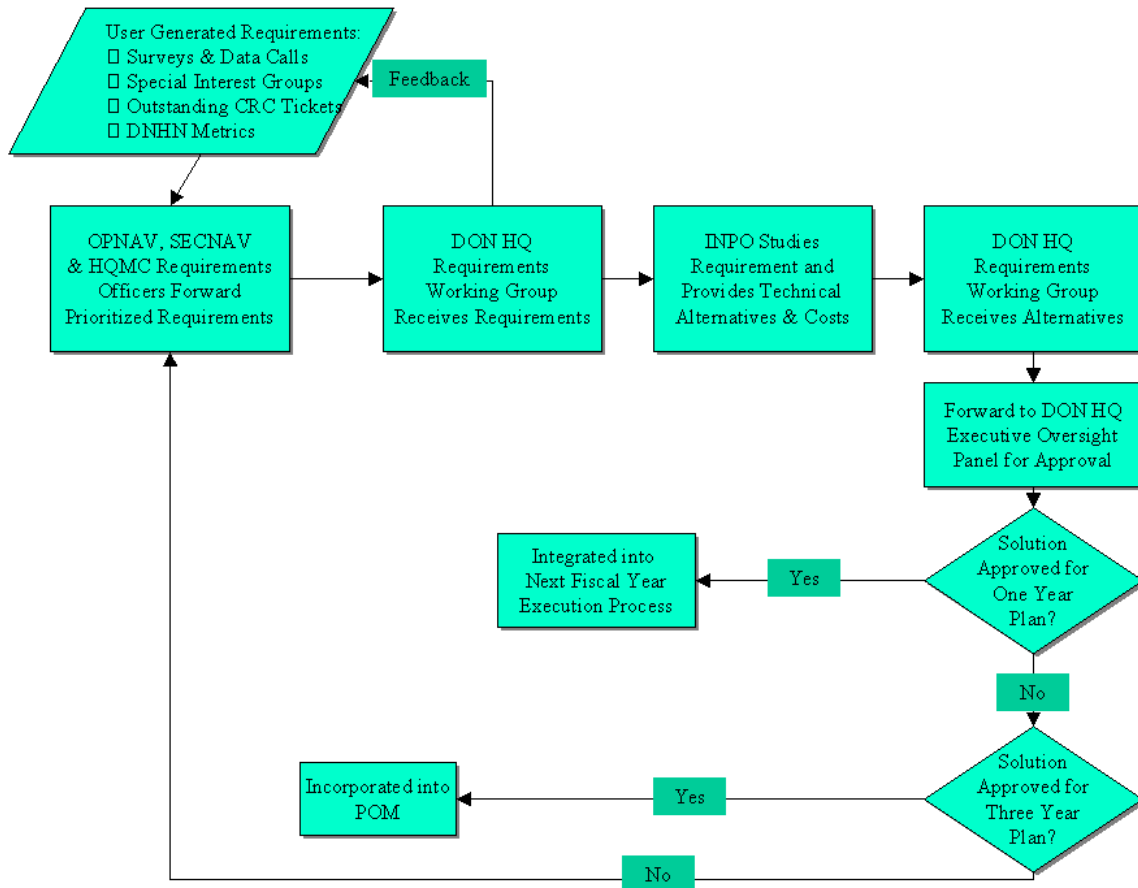
- 1) Take a flushed or used diskette from the “**Toolbox**” stock of diskettes.
- 2) Ensure Write Protect tab on disk is down/closed.
- 3) Insert diskette into the disk drive of the CLASS PC.
- 4) Make sure your target file(s) are in a File Manager directory. (e.g., if your file is a cc:Mail attachment, you must File/Save As the file to a directory on the PC’s hard drive.
- 5) Execute TOOLBOX icon from the Global Apps window in Program Manager. (Note: Until installed in the Global Apps window, application is available at *G:\toolbox.*)
- 6) From the Toolbox main menu, highlight Secure Copy with the arrow keys, press Enter.
- 7) Enter S to change source drive (i.e., C:, H:, I:, O:, etc.)
- 8) To change directories, use arrow keys, then enter C.
- 9) Enter T to change the target drive (i.e., A or B).
- 10) Highlight desired file(s) using arrow keys and spacebar.
- 11) Press F10 to begin the copy process.
- 12) After copying, press Escape to exit, or change directory to copy more files.
- 13) Press F1 at any time for HELP.
- 14) From the Toolbox main menu, highlight Buster with the arrow keys, press Enter.
- 15) Indicate disk drive (A or B) when prompted.
- 16) The “Buster” utility will show you a list of “dirty words” it is checking for. Press Enter to begin.
 - a) The “Buster” utility will stop and highlight surrounding text each time it finds a dirty word on the disk. Press Enter to continue. It is your responsibility to determine whether the information is indeed classified (e.g., Buster will find “secret” inside the word “secretary”) and to not use the disk on the UNCLAS LAN if any classified information is found on the disk. (Note: “Buster” checks not only the file you are currently copying, but also any files which have been on the disk (even if they have been deleted).

- b) If the diskette busts clean, proceed with the next step. If not, put a red SECRET label on the disk and give it to your ADPSSO or run Norton WIPEINFO on it yourself. Restart your file copy from the beginning with another “Toolbox ” diskette.
- c) Take disk to UNCLAS PC and copy the file where you need it.
- d) Return the disk to the “**Toolbox** ” stock.

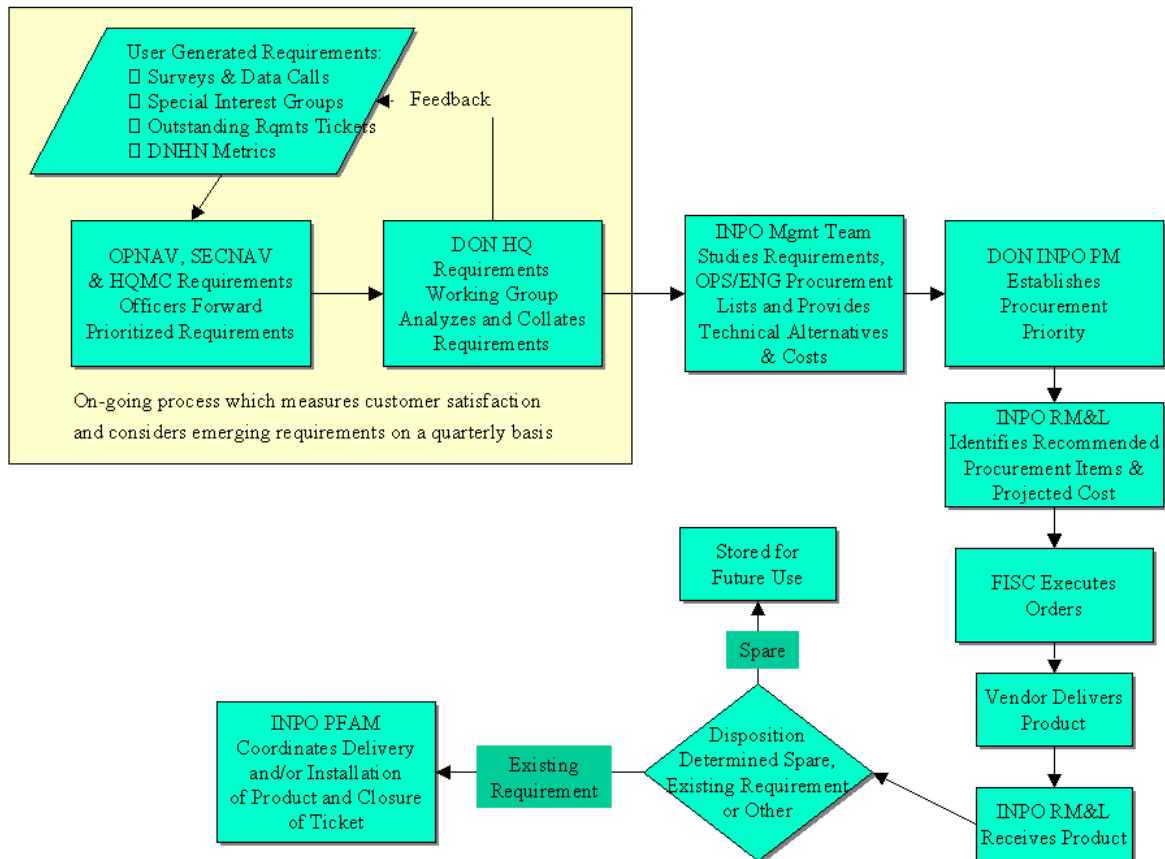
4.7.3 Flushing “Toolbox” Diskettes

- 1) Flush takes about seven minutes per diskette to run.
- 2) Insert diskette into the appropriate disk drive on the CLASS PC.
- 3) Execute TOOLBOX icon from the Global Apps window in Program Manager.
- 4) Indicate the correct drive (A, or B) when prompted.
- 5) Respond Yes to both “Do you want to...” questions, then Enter to start Flush.
- 6) Recommend that the Flush date be marked on the diskette label.
- 7) Return flushed disk to “**Toolbox**” stock.
- 8) Repeat for additional disks to be flushed.

APPENDIX F: REQUIREMENTS PROCESS--THREE-YEAR POM



APPENDIX G: REQUIREMENTS PROCESS—ANNUAL BASIS



APPENDIX H: REQUIREMENTS PROCESS--EMERGENT REQUIREMENTS

